

Índice de contenido

Manual OpenLdap como libreta de direcciones.....	2
Introducción.	2
1.Instalación de paquetes.....	2
1.Configuración Básica.....	2
2.Generar contraseña de Administrador para nuestro servidor Openldap.....	3
3.Archivo de configuración ldap.....	4
4.Ingresar datos al directorio ldap.....	6
5.Agregar Usuario.....	8
6.Configurar Outlook 2007.....	10

Manual OpenLdap como libreta de direcciones

Introducción.

LDAP (Lightweight Directory Access Protocol) es un protocolo para consulta y modificación de servicios de directorio que se desempeñan sobre TCP/IP. LDAP utiliza el modelo X.500 para su estructura, es decir, se estructura árbol de entradas, cada una de las cuales consiste de un conjunto de atributos con nombre y que a su vez almacenan valores.

1. Instalación de paquetes

Se debe realizar la instalación de los paquetes `openldap`, `openldap-clients` y `openldap-servers`, utilizando el siguiente comando:

```
[root@localhost ~]# yum -y install openldap openldap-clients openldap-servers
```

```
=====
Package           Arch      Version           Repository        Size
=====
Installing:
openldap-clients   i386      2.3.43-12.el5_5.2 updates          217 k
openldap-servers   i386      2.3.43-12.el5_5.2 updates          3.1 M
Transaction Summary
=====
Install      2 Package(s)
Upgrade      0 Package(s)

Total download size: 3.3 M
Downloading Packages:
(1/2): openldap-cl (4%) 62% [===== ] 99 kB/s | 136 kB  00:00 ETA
=====
```

Instalación de paquetes para openldap

Tras finalizar la instalación podremos consultar los siguientes manuales de ayuda de openldap.

Manuales de ayuda		
ldap	slapd	slapcat
ldap.conf	slapd.conf	slapadd
ldapadd	slapd.access	slappasswd
lapdsearch	slapdtest	ldif

Para utilizar los manuales de ayuda se debe ejecutar el comando `man` (nombre del manual) ej:

```
[root@localhost ~]# man ldap
```

1. Configuración Básica

En este paso vamos a crear el directorio donde almacenaremos los archivos de configuración de nuestra libreta de direcciones en nuestra carpeta `ldap` el directorio `addressbook`. Para ello utilizaremos el comando `mkdir` de la siguiente manera:

```
[root@localhost ~]# mkdir /var/lib/ldap/addressbook
```

Posterior a esto, se deben otorgar los permisos a la carpeta creada para que el usuario `Ldap` pueda escribir sobre la carpeta, eso se hace utilizando el siguiente comando:

```
[root@localhost ~]# chmod 700 /var/lib/ldap/addressbook/
```

Ahora nos ubicamos en nuestra carpeta ldap para ver su contenido

```
[root@localhost ~]# cd /var/lib/ldap/
```

```
[root@localhost ldap]# ls -l
```

Para cambiar el propietario de la carpeta se utiliza la siguiente línea:

```
[root@localhost ldap]# chown ldap:ldap /var/lib/ldap/addressbook/
```

Verificamos que la carpeta Addressbook ya cambio de propietario a ldap y esta carpeta a su vez tenga los permisos asignados anteriormente

```
[root@localhost ldap]# ls -l
```

Copiamos el archivo etc/openldap, adicionalmente vamos a realizar una copia del archivo de configuración de base de datos

```
[root@localhost ldap]# cd /etc/openldap/
```

en esta carpeta hacemos copia del archivo DB_CONFIG.example en nuestra carpeta addressbook creada recientemente pero lo dejamos con el nombre DB_CONFIG

```
[root@localhost openldap]# cp /etc/openldap/DB_CONFIG.example /var/lib/addressbook/
```

DB_CONFIG

```
[root@localhost ~]# mkdir /var/lib/ldap/addressbook
[root@localhost ~]# chmod 700 /var/lib/ldap/addressbook/
[root@localhost ~]# cd /var/lib/ldap/
[root@localhost ldap]# ls
addressbook  openldap-severs-update.log
[root@localhost ldap]# ls -l
total 16
drwx----- 2 root root 4096 sep 12 18:18 addressbook
-rw-r--r-- 1 root root 148 sep 12 17:50 openldap-severs-update.log
[root@localhost ldap]# chown ldap:ldap /var/lib/ldap/addressbook/
[root@localhost ldap]# ls -l
total 16
drwx----- 2 ldap ldap 4096 sep 12 18:18 addressbook
-rw-r--r-- 1 root root 148 sep 12 17:50 openldap-severs-update.log
[root@localhost ldap]# cd /etc/openldap/
[root@localhost openldap]# ls
cacerts  DB_CONFIG.example  ldap.conf  schema  slapd.conf
[root@localhost openldap]# cp /etc/openldap/DB_CONFIG.example /var/lib/ldap/
logrotate.status
[root@localhost openldap]# cp /etc/openldap/DB_CONFIG.example /var/lib/ldap/addressbook/DB_CONFIG
[root@localhost openldap]#
```

2. Generar contraseña de Administrador para nuestro servidor Openldap

Iniciamos con el siguiente comando

```
[root@localhost openldap]# slappasswd
```

asignamos la contraseña para el administrador del servidor Openldap

New password:

Re-enter new password:

Posteriormente nos va a generar una clave con un metodo de encriptación SSHA el cual podemos cambiar el tipo de encriptacion como el md5, SSHA o cript para este caso utilizaremos md5 de la siguiente manera

```
[root@localhost openldap]# slappasswd -h {md5}
```

Nuevamente ingresamos la nueva contraseña

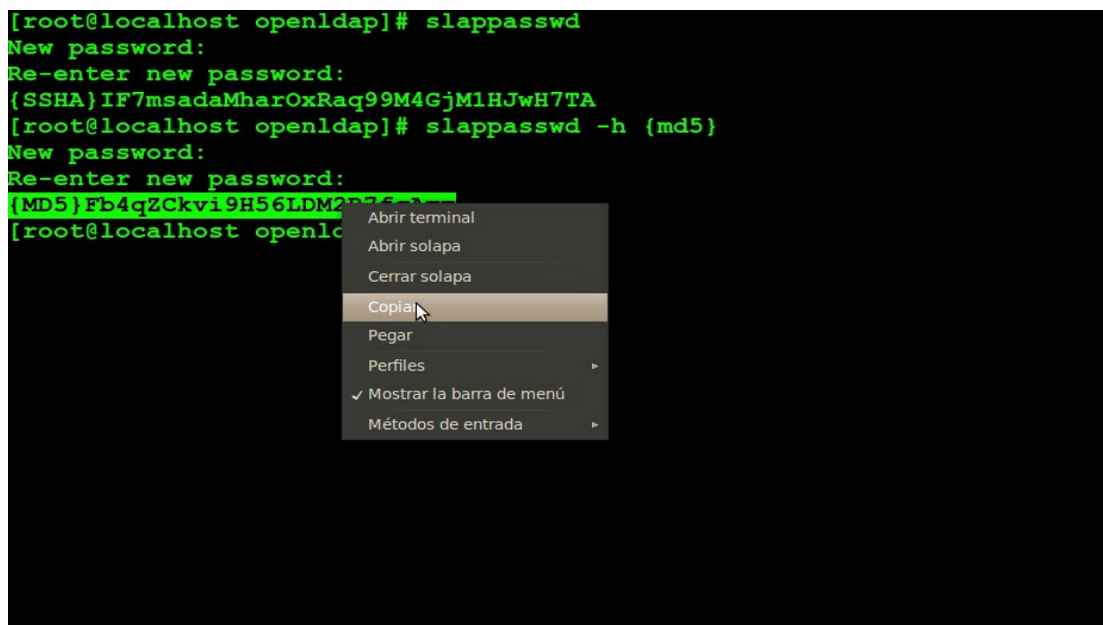
New password:

Re-enter new password:

Nos va a generar una nueva clave con el metodo de encriptación md5 Ejemplo:

{MD5} Fb4qZCkvi9H56LDM2R7fqA==

Copiamos esta nueva clave en un block de notas la cual utilizaremos posteriormente en nuestro archivo de configuración



```
[root@localhost openldap]# slappasswd
New password:
Re-enter new password:
{SSHA}IF7msadaMharOxRaq99M4GjM1HJwH7TA
[root@localhost openldap]# slappasswd -h {md5}
New password:
Re-enter new password:
{MD5}Fb4qZCkvi9H56LDM2R7fqA==
[root@localhost openldap]#
```

3. Archivo de configuración ldap

Con la clave que generamos en el paso anterior para el administrador Openldap vamos al archivo de configuración de ldap y lo configuramos

```
[root@localhost openldap]# cd /etc/openldap/
```

En esta carpeta debemos editar el archivo slapd.conf

```
[root@localhost openldap]# vi slapd.conf
```

```
[root@localhost openldap]# slappasswd -h {md5}
New password:
Re-enter new password:
{MD5}Fb4qZCkvi9H56LDM2R7fqA==
[root@localhost openldap]# cd /etc/openldap/
[root@localhost openldap]# ls -l
total 40
drwxr-xr-x 2 root root 4096 ago 11 08:19 cacerts
-rw-r----- 1 root ldap 921 ago 11 08:18 DB_CONFIG.example
-rw-r--r-- 1 root root 246 ago 11 08:19 ldap.conf
drwxr-xr-x 3 root root 4096 sep 12 17:50 schema
-rw-r----- 1 root ldap 3799 ago 11 08:19 slapd.conf
[root@localhost openldap]# vi slapd.conf
```

En el archivo de configuración debemos modificar los siguientes parámetros ubicando la línea en donde se encuentre:

en suffix modificamos el parámetro `dc` por nuestro dominio para nuestro ejemplo Hotfixed.net de la siguiente manera

suffix **"dc=hotfixed,dc=net"**

el rootdn es la cuenta de administración para nuestro openldap que para nuestro ejemplo es admin y también el nombre de dominio que es hotfixed.net de la siguiente manera

rootdn **"cn=admin,dc=hotfixed,dc=net"**

también debemos modificar nuestra contraseña para acceder al sistema la cual generamos anteriormente, en la línea rootpw modificamos la contraseña que esta asignada y copiamos la contraseña que generamos con el comando slappasswd la cual copiamos en un blog de notas recordemos borrar el `#` al inicio de la línea lo cual nos indica que es un comentario:

rootpw **{MD5} Fb4qZCkvi9H56LDM2R7fqA==**

Modificamos nuestro directorio configurando nuestra libreta de direcciones asignando la ruta donde se encuentra

directory **/var/lib/ldap/addressbook**

guardamos los cambios y cerramos el archivo con `:wq`

```
# ldbm and/or bdb database definitions
#####

database      bdb
suffix        "dc=hotfixed,dc=net"
rootdn        "cn=admin,dc=hotfixed,dc=net"
# Clear text passwords, especially for the rootdn, should
# be avoided. See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
# rootpw      secret
rootpw        {MD5}Fb4qZCkvi9H56LDM2R7fqA==

# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory     /var/lib/ldap/addressbook

# Indices to maintain for this database
index objectClass      eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid     eq,pres,sub
index nisMapName,nisMapEntry      eq,pres,sub
-- INSERT --
```

Finalmente iniciamos el servicio ldap

```
[root@localhost openldap]# service ldap start
```

configuramos el servicio para que arranque con el inicio del sistema con el comando:

```
[root@localhost openldap]# chkconfig ldap on
```

```
[root@localhost openldap]# slappasswd -h {md5}
New password:
Re-enter new password:
(MD5)Fb4qZCkvi9H56LDM2R7fqA==
[root@localhost openldap]# cd /etc/openldap/
[root@localhost openldap]# ls -l
total 40
drwxr-xr-x 2 root root 4096 ago 11 08:19 cacerts
-rw-r----- 1 root ldap 921 ago 11 08:18 DB_CONFIG.example
-rw-r--r-- 1 root root 246 ago 11 08:19 ldap.conf
drwxr-xr-x 3 root root 4096 sep 12 17:50 schema
-rw-r----- 1 root ldap 3799 ago 11 08:19 slapd.conf
[root@localhost openldap]# vi slapd.conf
[root@localhost openldap]# service ldap start
Verificando los archivos de configuración para slapd: config file testing succeeded
[ OK ]
Iniciando slapd:
[ OK ]
[root@localhost openldap]# chkconfig ldap on
[root@localhost openldap]#
```

4. Ingresar datos al directorio ldap

Ingresamos a la siguiente carpeta

```
[root@localhost openldap]# cd /var/lib/ldap/addressbook/
```

creamos un archivo ldif llamado addressbook.ldif con el comando:

```
[root@localhost addressbook]# vi addressbook.ldif
```

```
[root@localhost openldap]# cd /var/lib/ldap/addressbook/
[root@localhost addressbook]# vi addressbook.ldif
```

en el archivo creado vamos a generar los objetos dentro del archivo

iniciando por el nombre de dominio

dn: dc=hotfixed, dc=net

Posteriormente los atributos

objectclass: top

objectclass: dcObject

objectclass: organization

el parámetro nombre de la organización y nombre de dominio respectivamente

o:Hotfixed

dc: hotfixed

creamos otro objeto correspondiente a nuestra libreta de direcciones con nombre distinguido addressbook y su dominio htfixed.net

dn: ou=addressbook, dc=hotfixed, dc=net

creamos los siguientes atributos

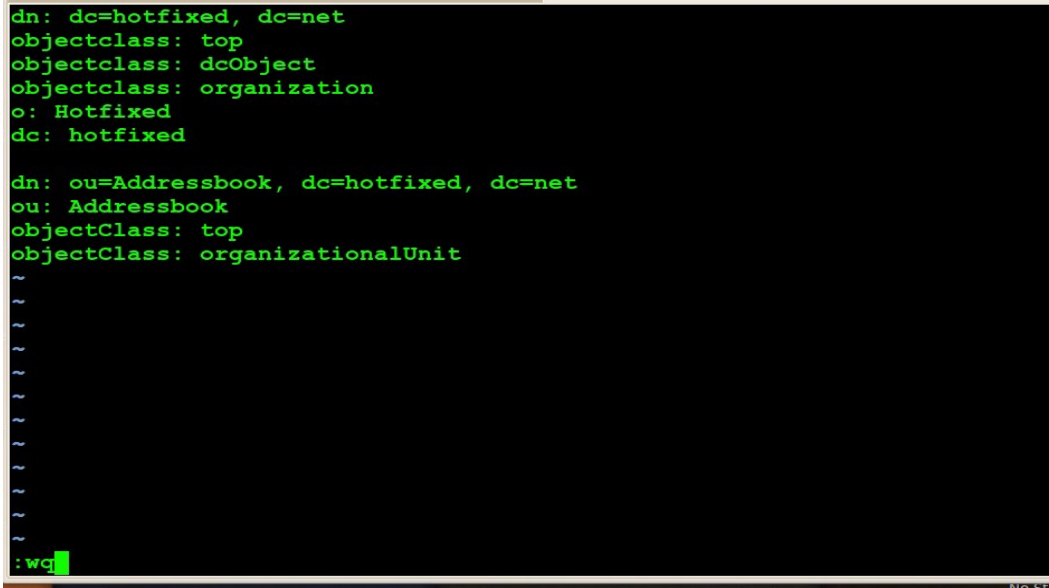
ou: Addressbook

objectclass: top

objectclass: organizationalUnit

Es importante dejar una linea de espacio entre los objetos para que no presente errores al reiniciar el servicio

Guardamos los cambios y cerramos con :wq



```
dn: dc=hotfixed, dc=net
objectclass: top
objectclass: dcObject
objectclass: organization
o: Hotfixed
dc: hotfixed

dn: ou=Addressbook, dc=hotfixed, dc=net
ou: Addressbook
objectClass: top
objectClass: organizationalUnit
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:wq
```

Añadimos estas entradas en nuestro servidor Openldap

[root@localhost addressbook]# ldapadd -x -W -D 'cn=admin, dc=hofixed, dc=ne' -h

- -x Autenticacion simple -h 127.0.0.1 -f addressbook.ldif
- -W al hacer esta entrada solicite contraseña
- -D Indicamos a nuestro comando ell nombre distinguido que vamos a usar para nuestro ejemplo admin y nuestro dominio hotfixed.net
- -h Cual es la dirección IP de nuestro servidor
- -f Archivo que vamos a utilizar para agregar la entrada

nos solicitara el password de administrador openldap el cual debemos ingresar

Si el archivo esta bien configurado y la contraseña es correcta aparecerá que se a agregado un nueva entrada con el nombre de dominio el cual es hotfixed.net y una nueva entrada con nuestra unidad organizacional que es addressbook.

```

[root@localhost openldap]# cd /var/lib/ldap/addressbook/
[root@localhost addressbook]# vi addressbook.ldif
[root@localhost addressbook]# ldapadd -x -W -D 'cn=admin, dc=hotfixed, dc=net' -h 127.0.0.1 -f addressbook.ldif
Enter LDAP Password:
adding new entry "dc=hotfixed, dc=net"

adding new entry "ou=Addressbook, dc=hotfixed, dc=net"

[root@localhost addressbook]# █

```

5. Agregar Usuario

Creamos un archivo ldif con el nombre de nuestro usuario para nuestro ejemplo Fabio Hernandez

```
[root@localhost addressbook]# vi fabio.ldif
```

En el archivo ldif agregamos los siguientes parámetros

Nombre distinguido(Fabio Hernandez), unidad organizacional a la que pertenece (addressbook) y dominio hotfixed.net

dn: cn=Fabio Hernandez, ou=addressbook, dc=hotfixed, dc=net

Posteriormente nuestros atributos

objectclass: top

objectclass: person

objectclass: organizationalperson

objectclass: inetOrgPerson

cn: Fabio Hernandez

givenName:Fabio

sn: Hernandez

displayName: Fabito "Nombre o apodo"

mail: Fabiohernandez@hotfixed.net "Correo Electrónico"

o: Hotfixed "Nombre de la compañía a la que pertenece"

ou: Informática "Nombre del departamento al que pertenece"

businessRole: Ingeniero de Soporte "Rol que desempeña en la compañía"

primaryPhone: 2259644 "Número de teléfono"

mobile: 315-330-0983 "Número de celular"

Podemos ingresar todos los atributos que necesitemos de nuestro usuario

Guardamos el archivo con :wq

```

dn: cn=Fabio Hernandez, ou=Addressbook, dc=hotfixed, dc=net
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: Fabio Hernandez
givenName: Fabio
sn: Hernandez
displayName: Fabito
mail: fabiohernandez@hotmail.net
o: Hotfixed
ou: Informatica
businessRole: Ingeniero de Soporte
primaryPhone: 2259644
mobile: 315-330-0983
~
~
~
~
~
~
:wq

```

Creamos una nueva entrada a nuestro servidor utilizando nuestro archivo pasando los datos de nuestra cuenta admin y nuestro dominio hotfixed.net

```
[root@localhost addressbook]# ldapadd -x -W -D 'cn=admin, dc=hotfixed, dc=net' -h 127.0.0.1 -f fabio.ldif
```

posteriormente nos solicitara la clave de nuestro servidor ldap la cual debemos ingresar

Aparecerá un error con el atributo bussiness rol porque no esta definido:

ldapadd: Undefined attribute type (17)

additional info: businessRole: attribute type undefined

Ingresamos a editar nuevamente nuestro archivo fabio.ldif

```
[root@localhost addressbook]# vi fabio.ldif
```

En nuestro archivo comentaríamos los atributos puesto que no tenemos ningún esquema en donde hallamos definido nuestros roles anteriormente con # al inicio de la línea y guardamos nuevamente los cambios con :wq

```

dn: cn=Fabio Hernandez, ou=Addressbook, dc=hotfixed, dc=net
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: Fabio Hernandez
givenName: Fabio
sn: Hernandez
displayName: Fabito
mail: fabiohernandez@hotmail.net
o: Hotfixed
ou: Informatica
#businessRole: Ingeniero de Soporte
#primaryPhone: 2259644
#mobile: 315-330-0983
~
~
~
~
~
~
:wq

```

Nuevamente debemos generar la entrada a nuestro servidor utilizando nuestro archivo e ingresando la clave de administrador del servidor ldap

```
[root@localhost addressbook]# ldapadd -x -W -D 'cn=admin, dc=hotfixed, dc=net' -h 127.0.0.1 -f fabio.ldif
```

Debe aparecer un mensaje que confirma que se ejecuto correctamente la entrada con los parámetros inicialmente definidos

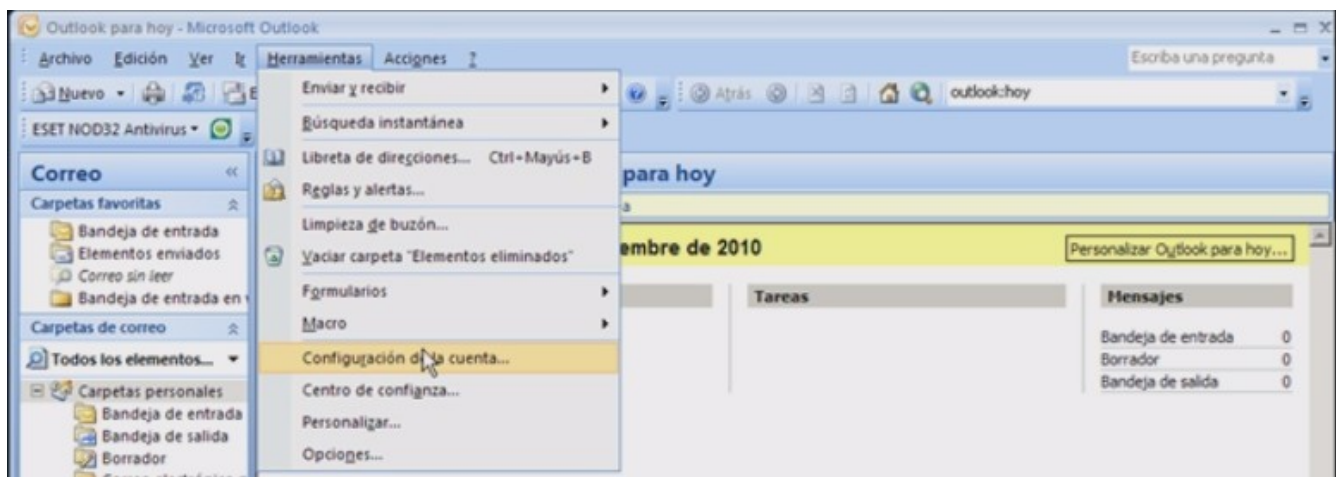
adding new entry "cn=Fabio Hernandez, ou=Addressbook, dc=hotfixed, dc=net"

```
[root@localhost addressbook]# vi fabio.ldif
[root@localhost addressbook]# ldapadd -x -W -D 'cn=admin, dc=hotfixed,
dc=net' -h 127.0.0.1 -f fabio.ldif
Enter LDAP Password:
adding new entry "cn=Fabio Hernandez, ou=Addressbook, dc=hotfixed, dc=net"
ldapadd: Undefined attribute type (17)
        additional info: businessRole: attribute type undefined

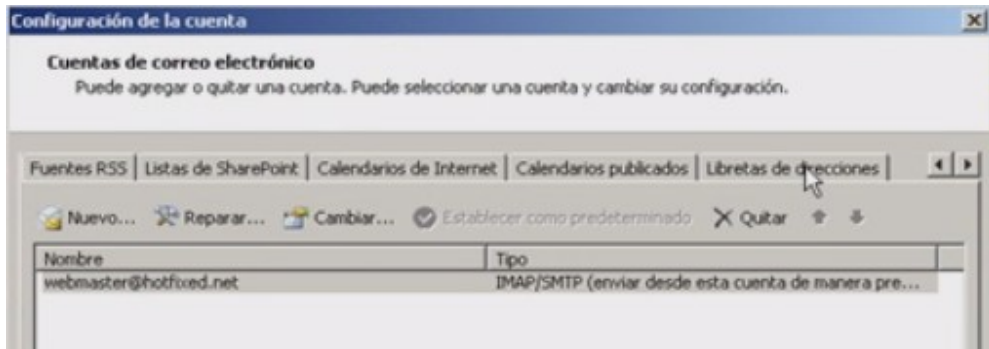
[root@localhost addressbook]# vi fabio.ldif
[root@localhost addressbook]# ldapadd -x -W -D 'cn=admin, dc=hotfixed,
dc=net' -h 127.0.0.1 -f fabio.ldif
Enter LDAP Password:
adding new entry "cn=Fabio Hernandez, ou=Addressbook, dc=hotfixed, dc=net"
[root@localhost addressbook]#
```

6. Configurar Outlook 2007

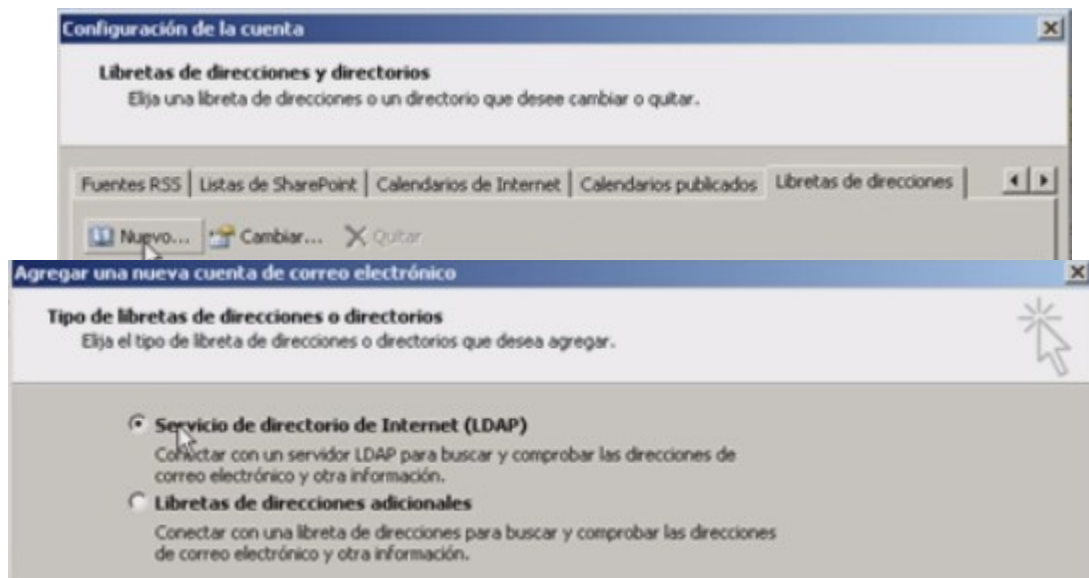
Para configurar Outlook 2007 contra el servidor openLdap. Vamos a Herramientas, Configuración de la cuenta.



Seleccionamos la pestaña Libreta de direcciones.



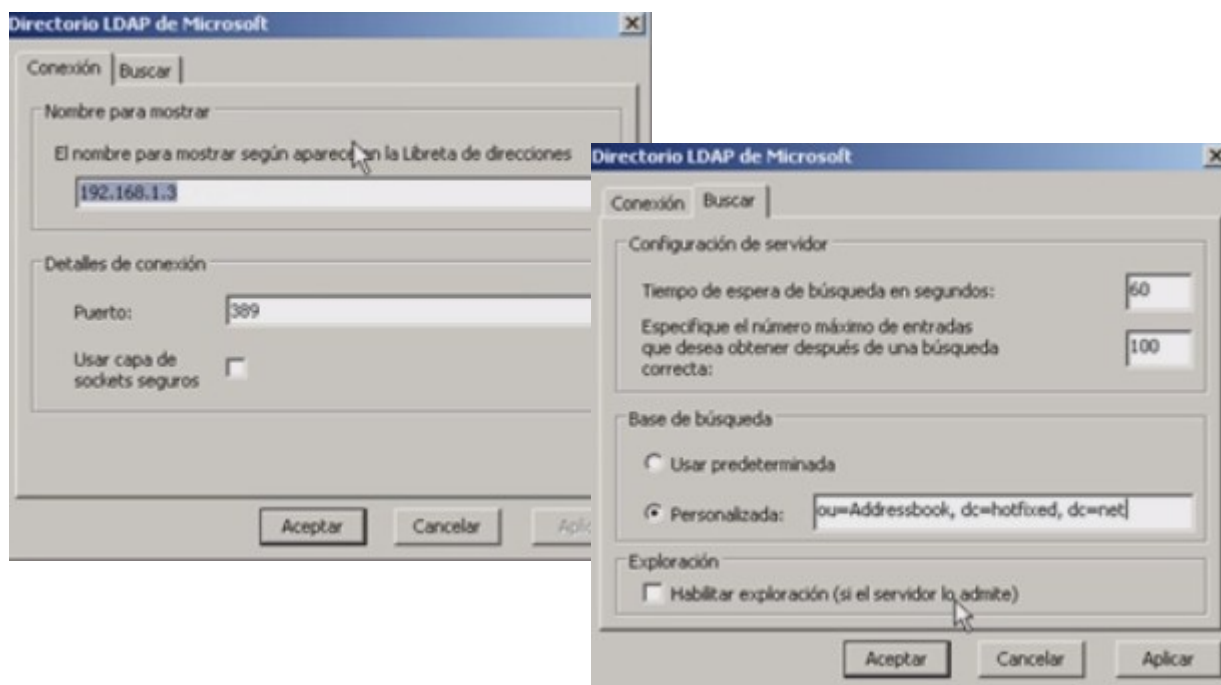
Luego damos click en el botón Nuevo y seleccionamos la opción Servicio de directorio de Internet (LDAP)



En la información del Servidor colocaremos el Nombre o dirección ip de el servidor, seleccionamos la opción El servidor necesita que inicie sesión y colocamos el nombre de usuario de nuestro servidor, en este caso cn=admin, dc=hotmail, dc=net y la contraseña correspondiente. Luego damos click en Mas configuraciones.



En la pestaña conexión verificamos la ip del servidor y el puerto 389, en la pestaña buscar, podemos establecer la base de búsqueda para este caso ou=Addressbook, dc=hotfixed, dc=net. Luego damos click en Aceptar y Reiniciamos el Outlook.



Al iniciar Outlook vamos a Herramientas, Libreta de direcciones, allí seleccionaremos la libreta que añadimos.

